Received: Added at production | Revised: Added at production | Accepted: Added at production

DOI: xxx/xxxx

RESEARCH ARTICLE

A Methodology for Cost-benefit Analysis of Information Security Technologies

Wen Zeng

Cyber Security Centre
School of Computer Science and Informatics
De Montfort University
Leicester LE1 9BH, U.K.
Email: wen.zeng.wz@gmail.com

Summary

Although information security technologies (such as digital rights management products) has been proven effective and successful in protecting the confidentiality of sensitive information by providing access control, these technologies have not been widely adopted and used to their potential. One reason for this could be that cost and benefit of these products have not been analysed in a systematic and quantitative manner to date. As a result, companies do not have an established procedure to evaluate the cost and benefit of implementing these products. In this document, the benefits of implementing a digital rights management product in enterprises are quantified using stochastic Petri nets models and are compared with the security needs of a corporation and potential costs incurred by the implementation process. An evaluating procedure for implementing these products is established. This procedure has the potential to be used to improve the ability of a corporation to make sensible security investment decisions.

KEYWORDS:
Information rights management, stochastic Petri nets, cost-benefit analysis, security metrics, human behaviour

1 | INTRODUCTION

Many organizations maintain sensitive information or documents that should be accessed only by authorized personnel, for example, personal health records in health institutions, bank statements and account balances for financial organizations. Confidential information leakage and sensitive information distortion have been identified as one of the major information security threats that cause reputation damage, identity theft and even threaten the viability of the company [1,2,3]. It is essential that companies and organizations keep these information and documents safe. Enterprise information security technologies, e.g., Digital Rights Management (DRM) systems, which are developed to address these concerns, use encryption to restrict the access of protected information and documents to authorized end users.

Enterprise information security technologies were introduced in the 1990s [4], however, they have not been widely implemented and used to its full potential. The investment into an enterprise information security product involves massive uncertainty. Therefore, one major hurdle for implementing these products maybe that organization, as potential users, do not have an established procedure to evaluate the benefit, effectiveness, impact and cost of these products quantitatively.

Enterprise information security research has been traditionally focused on the technologies and products themselves, for example, the architectures of system [5], access control policies [6,7,8,9,10], the functionality of products [11]. The impact of these products on business processes and the impact of human behaviour on the effectiveness of information security system have not been

documented to date, although human behaviour has been identified as one of the critical factors that determine the effectiveness of security measures [12,13].

There has not been an established systematic approach or procedure to quantitatively evaluate the project economics of information security technologies, including their effectiveness, benefits and costs to organizations, although information security researchers proposed various methods for addressing security investment problems. For example, in [14], the author proposed that we should consider the costs of subsequent maintenance of the software products, and pointed out that real-world failures of security protocols may sometimes be explained by economics [14]. However, this study did not point out any methodology to solve these problems. In [15], the authors considered that large system failures cost industry billions, thus, we need a better understanding of what sort of institutions can best evolve and manage large complex interconnected systems. In addition, the authors introduced a novel framework for analysing information security problems. However, this study did not mention any mathematical model to analyse this framework. In [16,17], the authors used mathematical models and stochastic simulations to examine the effectiveness of security operation processes and protection mechanisms. In [18], the authors proposed to use economic models based on trade-off between information confidentiality, integrity and availability to assess the effectiveness and value of security investment of a system. However, in these studies, the authors did not consider the time loss in the organizations by implementing information security technologies. In [19], the authors used economic models to measure the security risks in contemporaneous businesses and organizations. However, this study did not consider the security metrics for analysing information security technologies. In [20,21,22,23], the authors provided a system security model from the perspective of an adversary using stochastic activity networks. However, the security metrics which were introduced in these studies focused on the adversary profile, they did not consider the implementation of information security technologies in the systems. In [24,25,26], the authors mentioned that we should consider the cost and benefit of implementing information security policies in cloud computing systems, and introduced security metrics to analyse the effect of security policies; however, they did not have a procedure to evaluate the benefit and cost of implementing information security policies.

The primary objective of this study is, therefore, to establish a standard procedure for organizations to conduct cost-benefit analyses for information security technologies using stochastic models. This procedure applies the concept of security metrics and stochastic Petri nets to simulate the business processes and human behaviour involved in the information security technologies. Potential cost and benefit of deploying information security products can be evaluated in quantitative terms. Using this procedure, not only different information security products can be compared in the same term, information security projects can also be compared with other projects in the organizations' portfolio in monetary terms. This information provides basis for organizations to make sound investment decisions.

This document is organized as follows: Section 2 will introduce the methodology and quantitative evaluation procedure to evaluate the information security technologies. Section 3 is the background on quantitative models. Section 4 is the Microsoft Information Rights Management (MS IRM) case study. Section 5 is conclusions.

2 | METHODOLOGY

The proposed evaluation procedure will focus on the following three aspects: the value or benefit that information security technologies can bring to the organization; the effectiveness of the information security technologies and factors that will impact the effectiveness; and finally, the cost and impact that information security technologies have on organizations.

In this procedure, information is treated as a business asset with varying levels of commercial values as introduced by [27,28]. Since it is usually difficult to measure the benefits of information security technologies directly, costs of information disclose or modification is measured instead to quantify the benefits as suggested by [29].

In addition, human behaviour is an integrated part in this proposed procedure. Stochastic Petri nets are used to simulate the behaviour and interactions of people who are involved within organizational functions. Human behaviour has been identified as one of the critical factors that determine the effectiveness of security measures [12,13,30]. For example, information security mechanism will not be effective, if individual employee does not comply with it or is not aware of it [13]. Company policies, e.g., the way documents are classified, affect the effectiveness of the information security technologies as well.

Finally, in this procedure, a method of quantitatively evaluating cost and impact of the information security technologies in monetary is proposed. Some costs associated with the information security technologies are tangible, for example, the capital expenditures on information security technologies and associated hardware, software and daily operational expenditures associated with maintenance. These tangible costs are readily to be accounted for in monetary terms. There are also some intangible

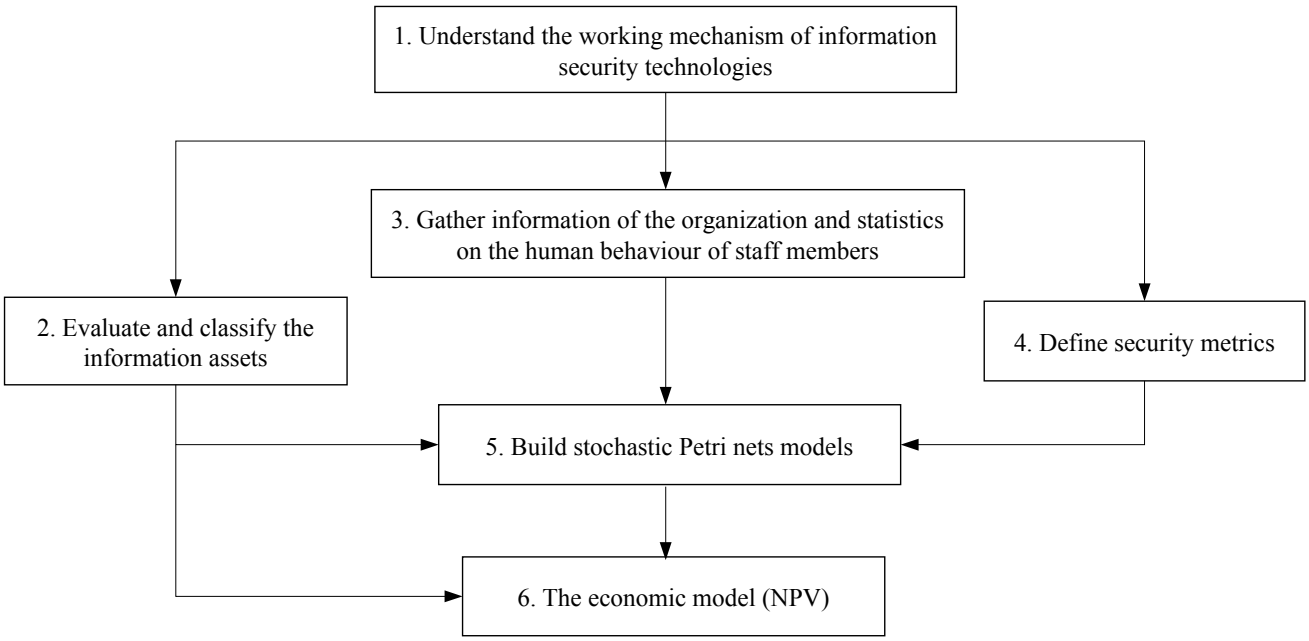

FIGURE 1 The flow chart of the proposed quantitative evaluation procedure (QEP) for information security technologies.

costs. For example, it has been documented that implementing a strict security mechanism will reduce the efficiency of the organization [13,31]. The request of security behaviour often has conflicts with and competes working hours with employee's production tasks [13]. In addition, encryption, a major function of information security technologies, often reduces the availability of data and brings inconvenience to end users to use protected documents [31]. The impact of information security technologies on staff productivity is quantified in terms of non-productive time (NPT) using the methodology proposed by [32,33,34,35].

The proposed procedure for quantitative evaluation of information security technologies is summarized in Figure 1 and described step by step below:

Step 1: Understand the working mechanism of the information security technologies in evaluation by testing the information security products and by reading manuals or white papers provided by the information security product providers. Plot flow charts, that represent the communications among users, servers, and administrators, will be created. These flow charts are the prototype of the business process.

Step 2: Evaluate and classify the organization's digital information assets. Study the organization's information classification policies, and classify the information into different categories by their level of confidentiality according to company policies. Then assign estimated values to digital information assets of each category. This information valuation process should be based on the business needs of the organization [28]. These values will be used in Steps 5 and 6 of this proposed procedure. Methods and processes to evaluate the value of documents can be found in published works, e.g., [28,36,37,38].

Step 3: Gather information of the organization and statistics on the human behaviour of staff members in the organization. These statistics include but not limited to: the total number of employees in the organization, the frequency that they use digital documents or information, the response time that a user has to wait to receive assistance from an administrator etc. It has been reported that most security incidents are caused by human errors instead of technology failures [39], although security incidents can result from nature disasters, technical issues and human acts [19]. Human acts can be further classified into two categories: malicious or non-malicious. Malicious acts often include different types of human malicious acts [13]. Non-malicious acts are usually caused by users who did not understand or ignored security policies. Typical violations include sharing of passwords and not closing documents after viewing them, and so on [19].

Three main techniques have been established and widely used to collect and analyse human behaviour data: questionnaires, interviews, and action research. A questionnaire consists of a series of questions; respondents answer questions by completing

the questionnaire themselves[40]. An interview is a conversation between the interviewer and the interviewee, in which interviewer elicit information from the interviewee[40]. Action research is a reflective process of progressive problem solving. Researcher themselves are actively involved in the topic being researched. They work with each other to improve the current situation[41]. In[42,43], the authors introduced action research methods into information systems research. In[44], the author successfully applied the action research method to evaluate the impact of information security awareness training on users' information security behaviour.

Human behaviour data are critical inputs into the stochastic Petri nets model in Step 5. It might take significant time and effort to gather this information; however, the better the quality of the statistics on user behaviour, the more accurate the results of the evaluation of the information security technologies will be. In general, if the model is more complex, more data are needed.

Step 4: Define security metrics. Security metrics are a series of criteria that are defined to help organization measure the success of security investments; security metrics enable organization to know how well the security products or security strategies are meeting the security objectives. Most security metrics cover these four different aspects: perimeter defense capability, coverage and control, availability and reliability, application risks[45]. The value of each item in the metrics will be generated by the stochastic model in Step 5.

For example, the number of digital documents protected by the DRM product is a measure of DRM product perimeter defense capability; the number of workstations covered by DRM product is the measure of the coverage of control of DRM product; the amount/percentage of documents that cannot be accessed by authorized users is a measure of the availability and reliability of the DRM product. The number of users who share password to open protected document is the measure of the application risks of the DRM product. For cloud computing systems, the value of opacity or diagnosability is the measure of information flow security after implementing security policies in the systems[24,46,25]. Information on choosing and defining security metrics can be found in previous publications, e.g.,[45,47].

Step 2, 3 and 4 can be executed concurrently, because one step can assist the others. For example, when we classify the organization's digital information assets, we should consider who are the main users of these information assets and what kind of security metrics we should use to evaluate the benefit or cost of implementing information security technologies to protect these assets.

Step 5: Build a stochastic Petri net model that includes a set of ordered activities to be undertaken by humans or other resources of the organization. This stochastic Petri net model is a structure for actions and implies on how work is done within an organization. These actions are work activities across time and space, with a beginning and an ending[48]. Users in the organization use digital information and documents to do their daily work. Information classification policies and human behaviour shapes the business process in the organization. After the stochastic Petri net model is constructed, parameters collected and defined in Step 3 is input into the model. Model outputs are used to calculate the security metrics that are defined in Step 4.

Step 6: Account all the tangible and intangible costs of information security technologies and calculate the Net Present Value (NPV) of information security technology implementation project using the results from Step 5. The calculated NPV is then used to help information security manager to make security investment decisions. Further information on NPV and economic model can be found in previous publications, e.g.,[29,49].

3 | BACKGROUND ON QUANTITATIVE MODELS

3.1 | Petri Nets Mechanism

The core part of the procedure proposed in this paper is Step 5, in which the stochastic Petri nets are applied to simulate the business processes in the organization. Stochastic Petri nets theory is introduced first in this section.

3.1.1 | Petri Nets

Petri nets are a graphical modelling tool for a formal description of systems whose dynamics are characterized by concurrency, synchronization, mutual exclusion and conflict[50,51]. In particular, they have been widely used for structural modelling of business processes and have been applied in a wide range of qualitative and quantitative analyses[50,52,53].

A basic Petri net N consists of two types of nodes, Pl and Tr, respectively called *places* and *transition*, a set $F \subseteq (Pl \times Tr) \cup (Tr \times Pl)$ of *arcs* that connect the nodes, and the initial marking $M_0 : Pl \to \mathbb{N}$ which is a mapping from the set of places to the set $\mathbb{N}$ of all non-negative integers.

Input arcs start at places and end at transitions, while *output arcs* start at transitions and end at places. Places can contain *tokens*, which are used to simulate the dynamic and concurrent activities of the system modelled by the net. The current state of the modelled system (a *marking*) is given by the number of tokens in each place.

Transitions are the active components of the net. When a transition is executed (or *fired*), it consumes tokens along its input arcs, and produces tokens along its output arcs. The resulting movement of the tokens changes the states of the system. A transitions is only allowed to fire when it is *enabled*, which means that each input place holds at least one token.

One can associate a firing delay with each transition of a Petri net; such a delay specifies the time that the transition has to be enabled before it can actually fire. If the delays are given by a random distribution function, we obtain a stochastic Petri net.

3.1.2 | Stochastic Activity Networks

Stochastic Petri nets extend the classic Petri nets with timing and probability features, and stochastic activity networks (SANs) are a class of stochastic Petri nets [54,55]. This permits the representation of both performance and dependability related characteristics, depending on the interpretation given to the tokens in the model.

SANs consist of four primitive objects: *Activities, places, input gates* and *output gates*. Activities ('transitions' in Petri net terminology) are two types, *timed* and *instantaneous*. Elongated ovals represent *timed activities* and solid bars represent *instantaneous activities*. Timed activities are used to represent activities of the modelled system, whose duration impact the system's ability to perform. Instantaneous activities represent system activities which, relative to performance variable in question, complete in a negligible amount of time. Places are depicted as circles and, as with Petri nets, each place can hold a non-negative number of tokens.

Cases (a generalization of probabilistic arcs) can be associated with both timed and instantaneous activities and are represented by small circles. Cases permit the realization of two types of spatial uncertainty. Uncertainty about which activities are enabled in a given marking is realized by cases associated with intervening instantaneous activities. Uncertainty about the next marking assumed upon completion of a timed activity is realized by cases associated with that activity. Input gates contain both an enabling predicate and input function (on the marking of the places). The enabling predicate must be true for the activity associated with that gate to be enabled. Upon completion of the associated activity, the input function is executed, possibly changing the marking of the net. Output gates have a single output function (on the marking of the places) associated with them, which is executed upon completion of the associated activity.

The stochastic nature of the nets is realized by associating an activity time distribution function with each of the timed activities and a probability distribution with each set of cases. In [32,33,34,35], the authors proposed to use the firing delay to model the NPT when users have to wait on the response from DRM administrators to help them with digital document access issues.

Reward models are used to specify measures of system behaviour. A reward model consists of a stochastic process and a reward structure. The stochastic process represents the dynamics of the system and can be constructed by hand or, automatically, from some network level description. The reward structure is typically a set of one or more functions defined on the states or transitions between states in the process.

A reward model in SANs has two different reward components: one is concerned with 'rate rewards', that is, the rate at which reward accumulates while the process is in a specified set of markings during an interval of time; and the other is concerned with 'impulse rewards', based on the count of the number of times an activity fires during an interval of time. The functions used to capture the activity and marking based rewards in a SAN, with places Pl and activities A, are given as follows:

- $C : A \to \mathbb{R}$. For each $a \in A$, $C(a)$ denotes the reward obtained due to the completion of activity a.
- $\mathcal{R} : \mathcal{P}(Pl, \mathbb{N}) \to \mathbb{R}$. For each $v \in \mathcal{P}(Pl, \mathbb{N})$, $\mathcal{R}(v)$ denotes the rate of reward obtained when for each $(pl, n) \in v$, there are n tokens in place pl.

where $\mathbb{N}$ is the set of natural numbers, and $\mathcal{P}(Pl, \mathbb{N})$ is the set of all partial functions from Pl to $\mathbb{N}$.

Impulse rewards are associated with activity completion (via C) and rates rewards are associated with the number of tokens in sets of places (via $\mathcal{R}$).

In the following, variable types of the interval category are denoted by 'Y' while variables types of the time-averaged category are denoted by 'W', each with the appropriate subscript. We let

$$Y_{[t,t+l]} = \sum_{v \in \mathcal{P}(Pl,\mathbb{N})} \mathcal{R}(v) \cdot J^{v}_{[t,t+l]} + \sum_{a \in A} C(a) \cdot N^{a}_{[t,t+l]} \qquad \& \qquad W_{[t,t+l]} = \frac{Y_{[t,t+l]}}{l}$$

In the above, the reward accumulated is related to the number of times each activity completes and time spent in particular markings, during a time interval $[t, t+l]$.

- $J^{v}_{[t,t+l]}$ is a random variable representing the total time that the SAN is in a marking such that for each $(pl, n) \in v$, there are n tokens in pl during $[t, t+l]$.
- $N^{a}_{[t,t+l]}$ is a random variable representing the number of completions of activity a during the interval $[t, t+l]$.

3.2 | Project Economics

For corporations and organizations to make sound decisions on the implementation of an information security system, all the associated costs and benefits over a multi-year period have to be taken into account. In this proposed procedure, the concept of net present value (NPV) from economics, project management and decision making science is adopted to quantify the value of an information security technology implementation project. NPV takes the time value of money into consideration. The basic concept is that money spent or obtained in the future will have a discounted value than money spent or obtained in the present[56]. NPV calculation is based on the principle of discounting; all the future cash flows are discounted back to the present time, which means one pound today is worth $(1+i)^t$ pound at time t in the future.

$$NPV = -K + \sum_{t=0}^{T} \frac{R_t - C_t}{(1+i)^t}$$

In which, $-K$ is a capital costs now (K at time zero), t is the time of the cash flow, R_t is the benefits return of year t, C_t is ongoing costs which is the cost of year t, i is the discount rate. Organizations usually have its own defined discount rate, although this discount rate is in general tied to the national interest rate.

NPV is one of the most widely used decision making criteria. If the NPV of a project is positive, this project will generate positive cash flow to the organization over a certain period, therefore, is beneficiary or profitable to the organization. However, when the capital of an organization with a portfolio of many profitable projects (NPV > 0) is constrained, not all the project with a positive NPV can be invested. The organization usually set a value larger than 0; projects with higher NPV usually have higher priorities for investment.

4 | MICROSOFT INFORMATION RIGHTS MANAGEMENT

In this section, Microsoft Information Rights Management (MS IRM) is studied in order to illustrate the procedure proposed. MS IRM is a DRM product developed by Microsoft Corporation. It is a Microsoft Office component, and can be implemented through the Rights Management Services (RMS) installed on Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, or to a cloud tenant with an Azure RMS subscription[57].

4.1 | MS IRM System Analysis

According to the proposed procedure, the first step is to understand the working mechanism of the information security products by reading the information security products user manual and by testing using the software. General information on the architecture, major components and major functionalities of DRM system is available in previous publications[58,59,60,61].

One key feature of the MS IRM is that MS IRM centrally manages documents and messages, and uses encryption to keep the information secure no matter where it has been transferred. Authorized users use decryption keys to open the document and access the information[57,62,63]. Administrators who have unlimited access to this centralized space play a key role in the IRM business process. Administrators manage protected documents or messages by defining and changing policies for all the documents or messages and authorized users regardless of the document location. Administrators create new authorized users or delete existing authorized users from the user list of the document or message[57,62]. The workflow of creating and viewing a protected document by authorized users is illustrated in Figure 2. When a user tries to open a protected document (process 7), the centralized server will check the authentication of the user. If the authentication fails, the user has to seek help from the administrator. The administrator will then check the identity of the user to make sure that the user has the status to access the document and add this user to the authorized user list of the particular document (processes 4 and 5).

The working mechanism in an MS IRM environment is described below:

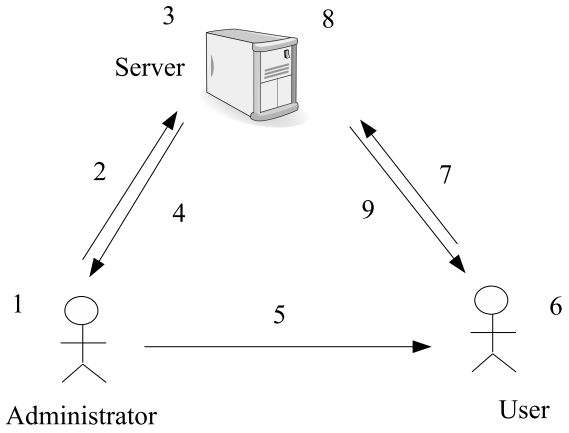

FIGURE 2 A simple representation of the working mechanism of MS IRM product. This chart illustrates the relationship between the MS IRM server, administrators, and users.

1. An administrator uses an IRM-enabled application to create a normal document or message. When the administrator chooses the restrict permission option, the IRM controller is triggered. The IRM controller immediately requests a username and a password from the administrator. When the administrator's response is sent to the server, the server validates the client. If the information is validated; the administrator can define users and users' rights for this document or message.
2. The IRM controller encrypts the document or message with a random symmetric key, and then sends a request for a publishing license directly to the IRM server. The request includes the random symmetric key, usage policies assigned to the encrypted document or message.
3. The IRM server encrypts the symmetric key with the server public key. Then the IRM server generates a publishing license, which includes the encrypted symmetric key, rights policy assigned to the encrypted document and the Uniform Resource Locator (URL) of the IRM server. IRM server then encrypts the publishing license with public key. Users and documents, rights and private key are kept in the IRM server.
4. The server returns the publishing license to the administrator side, and binds the publishing license to the encrypted document file.
5. Administrator distributes the document.
6. When a user tries to open an MS IRM protected document, the IRM controller is triggered on the user side, which requests the username and password information from this user.
7. The IRM controller sends a license request to IRM server. The license request includes the user's Rights Management Account Certificate (RAC), content identity, public key, publishing license, and the rights policy information.
8. The license generator on the server checks whether or not the user is authorized (the user's identity is present in the user identities repository). If the user's identity does not match the present identity in the identities repository, the server rejects creating use license. After the license generator confirms all the information, the license generator decrypts the symmetric key using the private key of the server, re-encrypts it using the public key of the user, and creates user license (which contains the symmetric key for decrypting the document and the rights information) for the user.
9. User license is sent back to client side, the IRM controller uses license to decrypt and open the encrypted document.

4.2 | Document Classification and Value

Documents or messages can be classified into many levels according to their confidentiality and the impact in the event their confidentiality is compromised[28]. In this case study, documents in the organization are divided into two levels: confidential and

unclassified documents. Users need a username and password to open confidential documents. It assumes that there are 4000 sensitive documents in the organization that need to be protected by MS IRM. 50% of sensitive documents in the organization are classified as confidential documents.

One reason for document classification is for practical purpose. It is often time-consuming and cost prohibitive to assign a value to each single document that needs to be protected. Once the document is classified, however, a single value can be assigned to a particular class. In this case study, the financial value of a confidential document is assigned to be £25, 000[28].

4.3 | User Behaviour Study

A set of assumptions on user behaviours are made (Table 1). In this table, the first five parameters: the number of authorized users in the organization, the number of documents that an authorized user might use every day on average, the number of normal working hours per day, the number of working weeks per year, and the number of administrators – these five parameters depend entirely on the size and business type of different organizations. Therefore, the values of these parameters are determined by literature based assumptions.

Other four parameters of the model can be gathered by previous research works and experiments. Average time service need to serve each user – the values of this parameter are the measurements from a real Google service[64]. Average time administrators need to help each user – this interview is taken in Newcastle University[33]. Average time users need to spend to pass user authentication – this experiment is taken in Newcastle University[33]. Percentage of time when authorized users experience a login system failure – this parameter is based on the experiment in University College London[65].

	Parameters	Value
1	Number of authorized users in the organization	50
2	Number of documents, a user might use every day on average	8
3	Number of normal working hours per day	8
4	Number of working weeks per year	52
5	Number of administrators in the organization	1
6	Average time service need to serve each user	0.01seconds
7	Average time administrators need to help each user	4.5 minutes
8	Average time users need to pass user authentication	7.33 seconds
9	Percentage of time when authorized users experience a login system failure and attempt ask administrator for help	0.70 %

TABLE 1 Data on human behaviour within the organization. Human behaviour is an important factor in the effectiveness of MS IRM. User behaviour data are critical input parameters of the stochastic Petri nets model. In general, they are gathered using questionnaire, interview, or action research methods.

4.4 | Security Metrics

Step 4 of this proposed procedure is to define security metrics in order to measure the confidentiality and availability of documents. MS IRM uses encryption to keep documents secure; this process decreases the availability of documents to unauthorized users. As discussed previously, the value of the implementation of MS IRM product is best measured by the cumulative value of all the confidential documents if they were disclosed to or modified by unauthorized users. The metrics for MS IRM are defined in Table 2.

	User's Type	Executive	Document Type
1	unauthorized	cannot read	unclassified
2	unauthorized	cannot read	confidential

TABLE 2 Security metrics defined to evaluate the effectiveness of the MS IRM system. It is in general difficult to measure the benefit of information security product. The potential cost when document is leaked or compromised is usually defined instead. The number of confidential and unclassified documents is therefore defined to evaluate the benefit of the MS IRM products.

4.5 | Stochastic Petri Nets Model Description and Results

Step 5 of the proposed procedure is to build a stochastic Petri net model and run this model. Data collected in Step 2, 3 and 4 are input into the stochastic Petri net model. The value of security metrics defined in Step 4 and the NPT will be generated by the simulation runs.

Potential users of a document can be classified into two groups, authorized user and unauthorized users. For confidential document, MS IRM requires users to log in using user's log-in ID and password. Authorized users should possess correct passwords to open documents that they have rights. However, authorized users might forget the password, because they might not open these documents frequently. In this case, the user will have to contact the administrator to retrieve the password. Administrators, however, are not always available, because they could be still handling previous requests. This will reduce the efficiency of the organization and will result in NPT[32].

For unauthorized users, since they do not suppose to possess the correct password, the chance for them to open a confidential document is reduced. However, unauthorized users might try a certain number of times and open the document successfully, or they might have acquired the correct passwords because of security leaks etc.

For authorized users, the main model objective is to quantify the reduction of working efficiency because of the changed workflow after installing MS IRM. As discussed previously, the NPT associated with the implementation of information security products is one of the main negative impacts on the organizations. In this proposed procedure, the NPT is modelled by timed transitions of stochastic Petri nets as proposed by Zeng and van Moorsel[32]. Two types of delays can be incurred by the implementation of MS IRM, the delay to pass authentication and the delay to wait for administrators' help.

Figure 3 shows the structure of a SAN model representing business process associated with MS IRM we discussed. The model consists of eight places, three timed transitions and three instantaneous transitions. Timed transitions are associated with random exponential distributed firing delays.

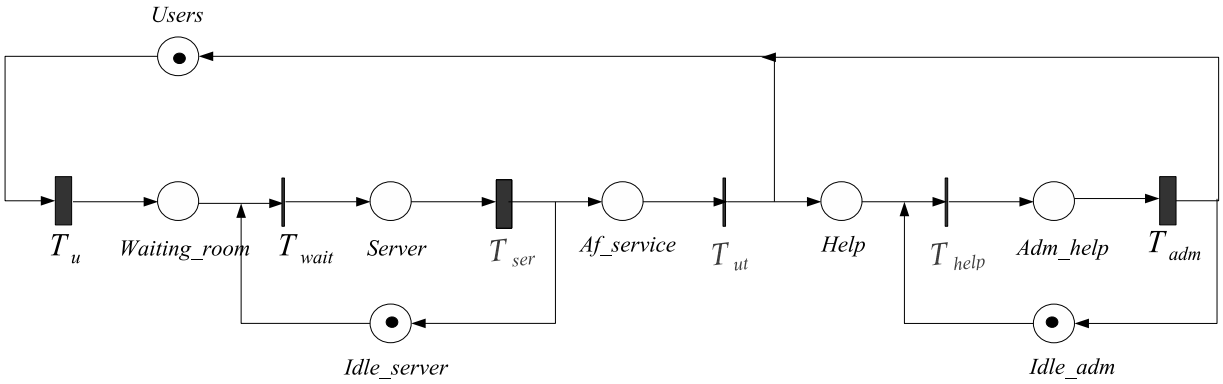

FIGURE 3 A SAN model of an MS IRM system. A SAN model consists of places, transitions, and arcs that connect them. In this figure, circles represent places, vertical lines represent transitions, and lines represent arcs. Note that the "thin" transition with output places takes no time to execute, i.e., it is instantaneous. Informally, the middle transition T_{ut} produces a token with in one of the two output places with probabilities p and $1 - p$, respectively.

Authorized users try to access protected resources every $\frac{1}{r_u}$ unit time. Place $Users$ contains the users that may arrive to the queue. The tokens in $Users$ are the authorized users. We use T_u to control the frequency of access requests sent by a user, thus

each completion of activity T_u represents the arrival of a request to the waiting room. Idle servers are represented by tokens in place $Idle\_server$, busy servers are represented by tokens in place $Server$. The time taken to access the protected resources is given by T_{ser}. The number of tokens in $Users$ represents the number of users who are trying to access resources, and the number of tokens in $Server$ represents the number of servers which are providing services to the users. In Figure 3, we have one black token in $Users$ and $Idle\_server$, if we want to increase the number of users or servers, we can increase the number of black tokens in these places.

If the user can pass the authentication process, then the user can use the resource; However, if the user cannot access the resource, the user has to contact the administrators for help. Place $Af\_service$ contains all users who went through the server, the probabilities on immediate transition T_{ut} represents the users passed the authentication process and the users did not pass the authentication process. Idle administrators are represented by tokens in place $Idle\_adm$, busy administrators are represented by tokens in place Adm_help. The time taken to help the users is given by T_{adm}. After obtaining such help, the user can try to access the resource again. If we want to increase the number of idle administrators, we can increase the number of black tokens in $Idle\_adm$.

We assume that there are one user, one idle server, and one idle administrator in the system. Figure 4 shows the corresponding reachability tree for the SAN model. The reachability tree has six nodes which represent six different states of the system. Increasing the number of users, servers and administrators will increase the state space of the system.

$$
\begin{aligned}
&M_0=\{1,0,0,1,0,0,0,1\}\\
&\quad\downarrow T_u\\
&M_1=\{0,1,0,1,0,0,0,1\}\\
&\quad\downarrow T_{wait}\\
&M_2=\{0,0,1,0,0,0,0,1\}\\
&\quad\downarrow T_{ser}\\
&M_3=\{0,0,0,1,1,0,0,1\}\\
&\quad\downarrow T_{ut}\\
&M_4=\{0,0,0,1,0,1,0,1\}\\
&\quad\downarrow T_{help}\\
&M_5=\{0,0,0,1,0,0,1,0\}\\
&\quad\downarrow T_{adm}\\
&M_6=\{1,0,0,1,0,0,0,1\}
\end{aligned}
$$

FIGURE 4 Reachability tree for the SAN model.

The behaviour of the SAN model can be measured by the *impulse rewards model* and *rate rewards model*, which are supported by the Möbius software[55]. The throughput of a transition is computed according to the formula which is described in Section 3.1.2,

$$\sum_{a\in A} C(a)\cdot N^a_{[t,t+l]}.$$

The number of tokens in sets of places is computed according to the formula

$$\sum_{v\in\mathcal{P}(Pl,\mathbb{N})} \mathcal{R}(v)\cdot J^v_{[t,t+l]}.$$

The time scale of the model is expressed in minutes, i.e., when we run the model one time unit in Möbius represents one minute in real working time.

To measure the throughput of the server, the throughput of a transition per unit of time T_{ser} was computed in average interval of time $[t, t + l]$. To measure the throughput of the administrator, the throughput of the transition per unit of time T_{adm} was computed in average interval of time.

We now put the parameters in Table 1 into the model in Figure 3, and run the model using the Möbius system[55]. From the result of this study, the deployment of the DRM product has a significant impact on the operational efficiency of the organization. Let us now consider one year of work after the deployment of the MS IRM in the network system of an organization, i.e., we consider 124800 time units in the SAN model (this corresponds to 52 weeks of work, each working week having 40 working hours). To measure the NPT, the time users spend in any place other than *Users* is computed. The NPT also includes the time the user takes for sending an access request ($\frac{1}{r_q}$).

Figure 5 shows the NPT of the system w.r.t. the number of users for various values of N (Number of confidential documents, a user might use every day on average). The NPT includes: the time spent on sending an access request and authentication procedures, and the time spent on waiting for a response from administrator. In addition, we also assume that there are 4 confidential documents are prevented from reading by unauthorized users.

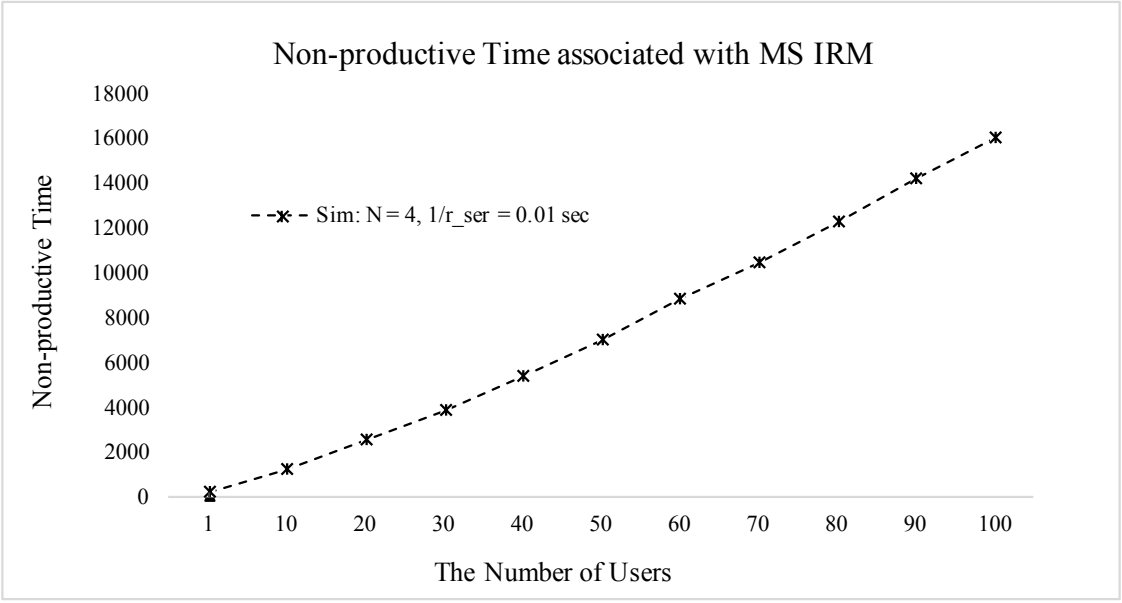

FIGURE 5 Total NPT associated with the deployment of MS IRM system. NPT increases significantly when the number of authorized users served by each administrator increases. The total NPT is composed of two components: the time loss associated with authentication process and the time loss associated with waiting on administrators when authorized users fail to pass the authentication process.

4.6 | Economic Model

In this section, the benefits and costs of implementing MS IRM products are compared using the concept of NPV.

As discussed previously, the benefit of the MS IRM system is the reduction in access of unauthorized users to confidential documents. In this case study, after using the MS IRM system for one year, we assume that 4 confidential documents are prevented from reading by unauthorized users. Use the assumed document value in Section 4.2, the annual benefits on documents disclosure amounts to £100,000 (Table 3).

The capital expenditure of implementing MS IRM system includes the purchase of MS IRM system itself and any associated costs to upgrade hardware and software. In addition, each year, 133.32 hours of NPT incurred as the result of the reduction in organizational efficiency after the implementation of the MS IRM system (Figure 5). In order to translate NPT into monetary

Annual Benefits Analysis on the Confidentiality of Documents by using MS IRM			
	Number of documents	Single document value	Total value
Confidential documents that are prevented from being read by unauthorized users	4	£25,000	£100,000
Total benefits	£100,000		

TABLE 3 Benefits analysis of the MS IRM product. The benefit of the MS IRM system includes a reduction in unauthorized access to confidential documents.

terms, the average salary of £60 per hour is used, therefore, in this study, the annual cost on NPT amounts to £7,999.2. For many projects, this is a conservative estimate, because of high daily operational rate, for example, the daily rates of drilling rigs in oil and gas industry. In addition, one administrator has to be hired to handle the MS IRM system and the requests in the organization. The average salary for an administrator or information security specialist is £42,296 per year[66]; therefore, the administrators' costs are around £42,296 per year. Training of employees in this case is assumed to cost £20,000 per year. The total costs associated with implementing MS IRM system is listed in Table 4.

Initial Capital Expenditure Costs by Deploying MS IRM	
Type of costs	Value
MS IRM software itself	£1,121.65
Upgrade hardware or operating system	£20,000
Total costs:	£21,121.65
Annual Operational Costs by Implementing MS IRM	
Type of costs	Value
Employee non-productive loss	£7,999.2
Administrator costs	£42,296
Training employees	£20,000
Total costs:	£70,295.2

TABLE 4 Costs analysis of the MS IRM product. The costs of MS IRM product include initial capital expenditure on MS IRM software and associated hardware and software upgrade cost. In addition, annual operational costs include administrator salaries, NPT associated with the reduction of operational efficiency and employee training costs.

The NPV of implementing the MS IRM can be calculated as following:

$$\begin{aligned} NPV\,at\,year\,one &= -K + \frac{R_1 - C_1}{(1+i)^1} \\ &= -£21,121.65 + \frac{£100,000 - £70,295.2}{(1+0.05)^1} = £7,168.64 \end{aligned}$$

$$\begin{aligned} NPV\,at\,year\,two &= -K + \frac{R_1 - C_1}{(1+i)^1} + \frac{R_2 - C_2}{(1+i)^2} \\ &= -£21,121.65 + \frac{£100,000 - £70,295.2}{(1+0.05)^1} + \frac{£100,000 - £70,295.2}{(1+0.05)^2} \\ &= £34,111.77 \end{aligned}$$

In which, R_t represents the benefit of year t; C_t represents the cost of year t; K is the initial capital expenditure. The discount rate i is assumed to be 0.05.

In this studied case, the NPV of implementing MS IRM is larger than 0. Therefore, the implementation project will bring positive cash flow to the organization. It is, therefore, recommended to implement MS IRM into the organization's network. However, as discussed previously, this is the optimal case, in which the capital of the organization is unconstrained. For an

organization with limited capital that has many profitable projects, projects with positive NPV will be compared against each other and the ones that have higher rate of return might be chosen to be invested.

5 | CONCLUSIONS

To assist security investors to make sensible investment decisions, a procedure that can quantitatively evaluate the benefits and costs of implementing information security technologies was established. The deployment of MS IRM system was used as a case study. In this example, the mechanism of MS IRM system is analysed; human behaviour of staff members in the organization is studied. A group of security metrics were developed to measure the effectiveness of the MS IRM system. Furthermore, the stochastic Petri nets are used to simulate and predict the impact of the deployment of the system on normal business processes. The simulation results provided important information that the business needed for making decisions on whether or not to implement this particular type of information security system.

This procedure was developed for the project in this particular case study under a set of assumptions; however, it has the potential to be used as a general practice during the procurement process of information security products. Different assumptions can be made and different parameters can be used based on the data collection of user behaviour study. These parameters are used in the stochastic model to tailor the needs and requirements of the security investor.

6 | ACKNOWLEDGEMENT

The author is very grateful to the anonymous reviewers for their detailed and constructive comments and suggestions.

References

1. Dolya A. Internal Threats Reports: Internal IT Threats in Europe 2006. 2007. https://securelist.com/internal-it-threats-in-europe-2006/36142/.
2. Gollmann D. *Computer Security*. New York, NY, USA: John Wiley & Sons, Inc. . 1999.
3. CESG . Security for Industrial Control Systems Manage the Business Risk, a Good Practical Guide. *Centre for the Protection of National Infrastructure (CPNI).* 2015.
4. Axelrod WC, Bayuk JL, Schutzer D. *Enterprise Information Security and Privacy*. Norwood, MA, USA: Artech House, Inc. 1st ed. 2009.
5. Spewak SH, Hill SC. *Enterprise Architecture Planning: Developing a Blueprint for Data, Applications and Technology*. Wellesley, MA, USA: QED Information Sciences, Inc. . 1993.
6. Bell DE. Concerning 'Modelling' of Computer Security. In: Proceedings. 1988 IEEE Symposium on Security and Privacy. ; 1988: 8-13.
7. Biba . Integrity Considerations for Secure Computer Systems. Tech. Rep. ESD-TR 76-372, MITRE Co.; 1977.
8. Denning R. *Cryptography and Data Security*. Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc. . 1982.
9. Denning DE. A Lattice Model of Secure Information Flow. *Communications of the ACM* 1976; 19: 236-243.
10. Goguen JA, Meseguer J. Security Policies and Security Models. In: 1982 IEEE Symposium on Security and Privacy. ; 1982: 11.
11. Allen J, Crabb G, Curtis P, Fitzpatrick B, Mehravari N, Tobar D. Structuring the Chief Information Security Officer Organization. tech. rep., Software Engineering Institute, Carnegie Mellon University; Pittsburgh, PA: 2015.
12. Adams A, Sasse MA. Users are not the Enemy. *Communications of the ACM* 1999; 42(12): 40-46.

13. Schneier B. *Secrets and Lies: Digital Security in a Networked World.* New York: Wiley Computer Publishing . 2000.

14. Anderson RJ. The Initial Costs and Maintenance Costs of Protocols. In: Security Protocols, 13th International Workshop, Cambridge, UK, April 20-22, 2005. ; 2005: 333-335.

15. Anderson RJ, Moore T. Information Security Economics - and Beyond. In: Advances in Cryptology - CRYPTO 2007, 27th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2007, Proceedings. ; 2007: 68-91.

16. Beres Y, Griffin J, Shiu S, Heitman M, Markle D, Ventura P. Analysing the Performance of Security Solutions to Reduce Vulnerability Exposure Window. In: Proceedings of the 2008 Annual Computer Security Applications Conference. IEEE Computer Society; Washington, DC, USA: 33-42.

17. Beres Y, Pym D, Shiu S. Decision Support for Systems Security Investment. *Manuscript, HP Labs* 2010.

18. Beautement A, Coles R, Griffin J, et al. *Modelling the Human and Technological Costs and Benefits of USB Memory Stick Security*: 141-163; Springer Science+Business Media . 2008.

19. Bojanc R, Jerman-Blazic B. An Economic Modelling Approach to Information Security Risk Management. *International Journal of Information Management* 2008; 28(5): 413-422.

20. LeMay E, Ford MD, Keefe K, Sanders WH, Muehrcke C. Model-based Security Metrics Using ADversary VIew Security Evaluation (ADVISE). In: Eighth International Conference on Quantitative Evaluation of Systems, QEST 2011, Aachen, Germany, 5-8 September. ; 2011: 191-200.

21. Ford MD, Buchholz P, Sanders WH. State-Based Analysis in ADVISE. In: Ninth International Conference on Quantitative Evaluation of Systems, QEST, London, United Kingdom, September 17-20. ; 2012: 148-157.

22. Ford MD, Keefe K, LeMay E, Sanders WH, Muehrcke C. Implementing the ADVISE Security Modeling Formalism in Möbius. In: 43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Budapest, Hungary, June 24-27. ; 2013: 1-8.

23. Rausch M, Feddersen B, Keefe K, Sanders WH. A Comparison of Different Intrusion Detection Approaches in an Advanced Metering Infrastructure Network Using ADVISE. In: Quantitative Evaluation of Systems - 13th International Conference, QEST, Quebec City, Canada, August 23-25, Proceedings. ; 2016: 279-294.

24. Zeng W, Koutny M, Watson P. Opacity in Internet of Things with Cloud Computing (Short Paper). In: 8th IEEE International Conference on Service-Oriented Computing and Applications, Rome, Italy, October. ; 2015: 201-207.

25. Zeng W, Koutny M, Watson P, Germanos V. Formal Verification of Secure Information Flow in Cloud Computing. *Journal of Information Security and Applications* 2016; 27-28: 103-116.

26. Zeng W, Germanos V. Benefit and Cost of Cloud Computing Security. *Harnessed Causality: Essays Dedicated to Maciej Koutny on the Occasion of His 60th Birthday* 2018: 143-150.

27. Huebner RA, Britt MM. Analyzing Enterprise Security using Social Networks and Structuration Theory. *Journal of Applied Management and Entrepreneurship* 2006; 11(3): 68-78.

28. Humphreys E. *Information Security Risk Management.* British Standards Institution . 2010.

29. Layard R, Glaister S. *Cost-benefit Analysis.* Cambridge: Cambridge University Press. 2 ed. 1994.

30. Davenport TH, Short JE. The New Industrial Engineering: Information Technology and Business Process Redesign. *Sloan Management Review* 1990; 31: 11-27.

31. Foroughi A, Albin M, Gillard S. Digital Rights Management: a Delicate Balance between Protection and Accessibility. *Journal of Information Science* 2002; 28(5): 389-395.

32. Zeng W, Moorsel vA. Quantitative Evaluation of Enterprise DRM Technology. *Electronic Notes in Theoretical Computer Science* 2011; 275: 159-174.

33. Zeng W, Liu K. Sensitivity Analysis of Loss of Corporate Efficiency and Productivity Associated with Enterprise DRM Technology. In: 7th International Conference on Availability, Reliability and Security. ; 2012: 445-453.

34. Zeng W, Liu K, Koutny M. Cost-benefit Analysis of Digital Rights Management Products using Stochastic Models. In: Proceedings of the 46th Annual Simulation Symposium, San Diego, CA, USA, April. ; 2013: 1.

35. Zeng W, Koutny M, Moorsel vA. Performance Modelling and Evaluation of Enterprise Information Security Technologies. In: 14th IEEE International Conference on Computer and Information Technology, Xi'an, China, September. ; 2014: 504-511.

36. Cavusoglu H, Mishra B, Raghunathan S. The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. *Journal of Electronic Commerce* 2004; 9(1).

37. Gary A, Curtis J, Halper H. Quantifying the Financial Impact of IT Security Breaches. *Information Management & Computer Security* 2003; 11(2): 74-83.

38. Hoo KJS. *How Much is Enough? A Risk-management Approach to Computer Security*. PhD thesis. 2000.

39. Sasse MA, Ashenden DM, Lawrence D, Coles-Kemp L, Flechais I, Kearney P. Human Vulnerabilities in Security Systems. tech. rep., UCL; 2007.

40. Bryman A. *Social Research Methods*. Oxford University Press . 2001.

41. Coombes H. *Research using IT*. New York: PALGRAVE . 2001.

42. Baskerville RL. Investigating Information Systems with Action Research. *Communications of the Association for Information Systems* 1999; 2.

43. Baskerville RL, Wood-Harper AT. A Critical Perspective on Action Research as a Method for Information Systems Research. *Journal of Information Technology* 2001; 11(3): 235-246.

44. Stephanou A. The Impact of Information Security Awareness Training on Information Security Behaviour. tech. rep., University of the Witwatersrand; 2008.

45. Jaquith A. *Security Metrics: Replacing Fear, Uncertainty and Doubt*. Boston: Pearson Education. Inc. . 2007.

46. Germanos V, Haar S, Khomenko V, Schwoon S. Diagnosability under Weak Fairness. *ACM Transactions on Embedded Computing Systems* 2015; 14(4): 69:1-69:19.

47. Bartol N, Bates B, Goertzel KM, Winograd T. Measuring Cyber Security and Information Assurance. tech. rep., Information Assurance Technology Analysis Center; 2009.

48. Davenport TH. *Process Innovation: Reengineering Work through Information Technology*. Boston: Harvard Business School Press . 1993.

49. Campbell HF, Brown RPC. *Benefit-cost Analysis*. Cambridge: Cambridge University Press . 2003.

50. Marsan MA, Balbo G, Conte G, Donatelli S, Franceschinis G. *Modelling with Generalized Stochastic Petri Nets*. Wiley Series on Parallel Computing . 1995.

51. Murata T. Petri Nets: Properties, Analysis and Applications. *Proceedings of the IEEE* 1989; 77(4): 541-580.

52. Salimifard K, Wright M. Petri Net-based Modelling of Workflow Systems: An Overview. *European Journal of Operational Research* 2001; 134(3): 664-676.

53. Aalst v. dWMP. The Application of Petri Nets to Workflow Management. *The Journal of Circuits, Systems and Computers* 1998; 8: 21-66.

54. Sanders WH. *Construction and Solution of Performability Models Based on Stochastic Activity Networks*. PhD thesis. University of Michigan, 1988.

55. Sanders WH. Möbius User Manual. *University of Illinois* 2018.

56. Law MA. Using Net Present Value as a Decision-making Tool. *Air Medical Journal* 2004; 23(6): 28-33.

57. Microsoft . Plan Information Rights Management in Office 2013. November 20 2017. https://technet.microsoft.com/en-us/library/cc179103.aspx.

58. Umeh J. *The World Beyond Digital Rights Management*. The British Computer Society . 2007.

59. Pitkanen O, Valimaki M. Towards a Digital Rights Management Framework. In: IeC2000 Proceedings. ; 2000.

60. Becker E, Buhse W, Gunnewig D, Rump N. *Digital Rights Management: Technological, Economic, Legal and Political Aspects*. Berlin: Springer . 2003.

61. Subramanya SR, Yi BK. Digital Rights Management. *IEEE Potentials* 2006; 25(2): 31-34.

62. Beek vMH. *Comparison of Enterprise Digital Rights Management Systems*. PhD thesis. Radboud University Nijmegen, 2007.

63. Bertrand Y. *Access Control Policies and Companies Data Transmission Management*. Theses. Universite Cote d'Azur, 2017.

64. Dean J, Barroso LA. The Tail at Scale. *Communications of the ACM* 2013; 56: 74-80.

65. Brostoff S, Sasse MA. Ten Strikes and You're out: Increasing the Number of Login Attempts can Improve Password Usability. In: Proceedings of CHI 2003 Workshop on HCI and Security Systems. John Wiley; 2003.

66. PayScale . Information Security Specialist Salary (United Kingdom). PayScale Incorporation, January 7 2018. https://www.payscale.com/research/UK/Job=Information_Security_Specialist/Salary.